AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
(A) Third floor room located inside a residence at 168 Parkside Avenue, Syracuse, NY; (B) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media, further described in Attachment A

Case No. 5:18-MJ-287 (TWD)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
(A) Third floor room located inside a residence at 168 Parkside Avenue, Syracuse, NY; (B) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media, further described in Attachment A

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 2252A	Distribution, Receipt and Possession of Child Pornography;
18 U.S.C. Sections 2422(b)	Enticement or Attempted Enticement of a Minor

The application is based on these facts:
See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Michael Ball, Special Agent DHS
Printed name and title

Sworn to before me and signed in my presence.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE.

Date: May 25, 2018

Judge's signature

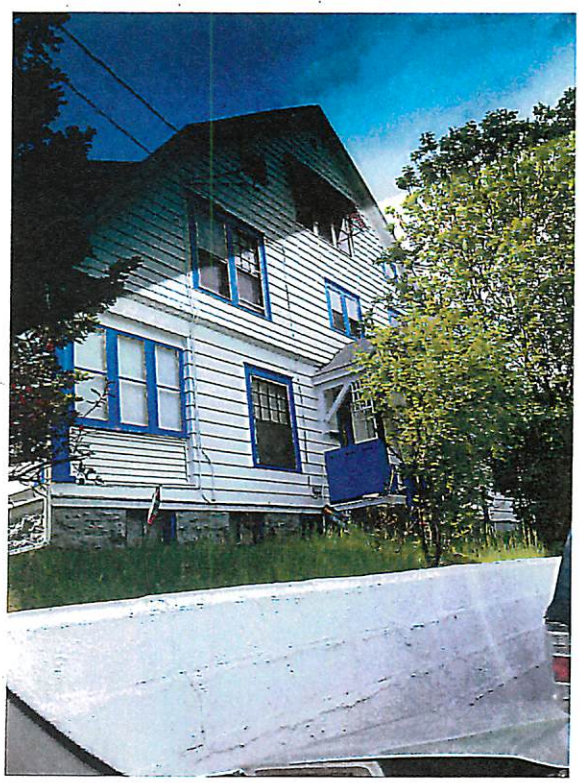
City and state: Syracuse, New York

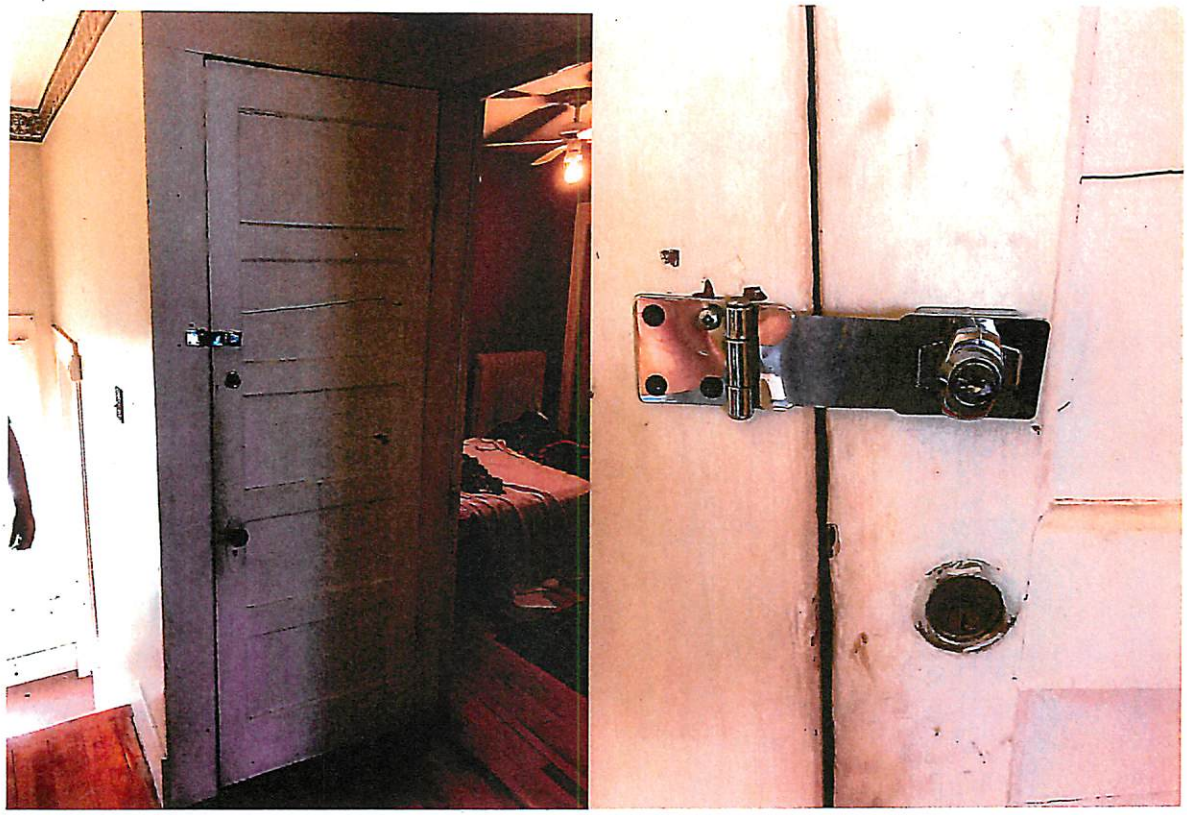
Hon. Thérèse Wiley Dancks, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A
PLACES AND ITEMS TO BE SEARCHED

The places and items to be searched are (A) Varrin's room which is located inside a residence at 168 Parkside Avenue, Syracuse, New York and (B) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media that are located during the course of said search.

The residence is described as a white with blue trim single family residence, located at 168 Parkside Avenue, Syracuse, New York. The residence is on the north side of Parkside Avenue, between Onondaga Avenue and Onondaga Park Drive. The driveway is on the east side of the residence. Entry is made into the house from the main entrance on the east side of the residence. Outside the main entrance is a small covered/open air porch. The main entrance has a white entry door which opens inward. Past the main door is a small foyer/mud room followed by a secondary door, which leads into the residence. Across from the secondary door is a carpeted stairway consisting of approximately ten (10) stairs, followed by a small landing. From the landing there is a second stairway facing the opposite direction of the first stairway, consisting of approximately five (5) steps which brings you to the second floor of the residence. The second floor consists of four (4) rooms and a stairway that leads to VARRIN'S room. The stairway has a white door with a hinged latch that is locked. The latch and lock are silver/chrome in color. The latch attaches to the door frame with three (3) black colored screws and one (1) silver/chrome colored screw, and attaches to the door with a locking mechanism.





ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items of evidence in violation of Title 18 USC §§ 2252 and 2252A (transporting, distributing, receiving, or possessing child pornography) and 2422(b)(enticement or attempted enticement of a minor) :

Computers and Electronic Media

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and electronic media will be conducted in accordance with the affidavit submitted in support of this warrant.

2. Computer hardware, meaning any and all computer equipment, including any electronic storing devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing, or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems, software, application software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data, whether themselves in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data, or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents and materials referencing or relating to the above described offenses. Such records, documents or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as thumb drives, flash drives, sd (secure digital) cards, floppy diskettes, hard disks, CD-ROMs, DVDs, optical disks, printer buffers, soft cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), or any computer or computer system. The form that such information might take includes, but is not limited to, thumb drives, flash drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, DVDs, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding, on computer media, or on media capable of being read by a computer or computer-related equipment, such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, removable hard disk cartridges, CDs, DVDs, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records

9. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored or maintained), books, notes, and reference materials.

10. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

11. Records of address or identifying information for the target of the investigation and any personal or business contacts or associates of his, (however and wherever written, stored or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user ID's, eID's (electronic ID numbers) and passwords.

12. Documents and records regarding the ownership and/or possession of the searched premises.

13. Computer records and evidence identifying who the particular user was who received, downloaded, possessed, or accessed with intent to view any child pornography found on any computer or computer media (evidence of attribution), or who attempted to do any of the foregoing, and how the computer was used to effectuate that activity.

Materials Relating to Child Erotica and Depictions of Minors

14. Any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors.

15. Any and all chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.

16. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18 United States Code, Section 2256(2).

17. Any and all notebooks and any other records reflecting personal contact, and any other activities, with minors who may be visually depicted while engaged in sexually explicit conduct, or engaged in sexually explicit chat, email, or other communications.

18. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, notes, and sexual aids.

19. Physical evidence related to the Subject Offenses, including, but not limited to clothing, personal belongings, and devices and articles which may be used to engage in sexually explicit conduct with minors

Materials Relating to Enticement of Minors

20. Any communications with minors or communications with adults regarding minors;

21. Any information pertaining to any individual's sexual interest in minors;

22. Any information in digital or hard-copy format regarding the use of Kidschat.net and the username "Prew654".

23. Any personal ads posted on any web site or in any physical newspaper or publication.

24. Any items, images, documents, communications, records, and information pertaining to the sexually explicit communications with minor(s) or adult(s) in relation to minors that

affected or were transmitted or received via computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail, including:

25. Envelopes, letters, and other correspondence including, electronic mail, chat logs, and electronic or. other instant messages, establishing possession, access to, effect on, or transmission through interstate or foreign commerce, including by United States mail or via computer, of child pornography or visual depictions of minors engaged in sexually explicit conduct;

26. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind affecting interstate or foreign commerce or involving the transmission via interstate or foreign commerce, including by U.S. mail or by computer, of any communications regarding a sexual interest in minors;

27. Credit card information, including bills and payment information, regarding Internet service; purchase of computer hardware, software, or storage media; purchase of or payment for memberships to web sites and/or chat applications;

28. Any items such as contraceptives that could be used to engage in sexual activity with a minor.

29. Any items that appear to be gifts for a young minor such as stuffed animals, flowers, that could be used to gain the minor's confidence and/or trust to induce a minor to engage in sexual activity.

30. Evidence identifying the location from which sexually explicit communications were held, including date and time of such communications;

31. Any and all photos or videos that may have been sent or received as part of a text or e-mail conversation relating to sexual interest in minors, to include date and time of the receipt or send of such files;

Photographs of Search

32. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

AFFIDAVIT

I, Michael J. Ball, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security (hereinafter "DHS"), Immigration and Customs Enforcement, Homeland Security Investigations (hereinafter "HSI"), assigned to the Resident Agent in Charge, Syracuse, New York. I have been so employed since April 2002. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography and the enticement of minors, in violation of Title 18, United States Code, Sections 2252, 2252A and 2422(b). During my tenure as a special agent, I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in Title 18, United States Code, Section 2256) in multiple forms of media, including computer media. I have participated in the execution of numerous search warrants, dozens of which involved child exploitation and/or child pornography offenses.

2. As will be shown below, there is probable cause to believe that Glenn Varrin has transported, received, possessed, or distributed child pornography, in violation of 18 U.S.C.§§ 2252 and 2252A and attempted to entice a minor in violation of 18 U.S.C.§§ 2422(b), and I submit this application and affidavit in support of a search warrant authorizing a search of (A) Glenn Varrin's room which is located inside a residence at 168 Parkside Avenue, Syracuse, New York and (B) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media that are located during the course of said search. Located within the places and items to be searched, I seek to seize evidence, fruits, and

instrumentalities of criminal violations relating to the knowing transportation, shipment, receipt, possession, and distribution, of child pornography, and the enticement or attempted enticement of minors as more particularly described in Attachment B.

3. As will be demonstrated in this affidavit, made under Fed. R. Crim. P. Rule 41, there is probable cause to believe that evidence will be located at the Subject Premises and within computers, computer equipment and/or other electronic media relating to violations of Title 18, United States Code 2252 and 2252A (transporting, distributing, receiving, or possessing child pornography) and Title 18, United States Code 2422(b) (enticement or attempted enticement of a minor), hereafter referred to as the Subject Offenses.

4. Since this Affidavit is being submitted for the limited purposes of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts and circumstances that I believe are necessary to establish probable cause to believe evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Sections 2252, 2252A and 2422(b) are presently located within the places and items to be searched.

BACKGROUND ON ELECTRONIC DEVICES AND CHILD PORNOGRAPHY

5. Based on my knowledge, training, and experience, and the experience and training of other law enforcement agents and investigators with whom I have had discussions, I know that electronic devices, including computers and cellular telephones serve different roles or functions with child pornography: production, communication, distribution, and storage.

6. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be

transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

7. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within recent years. These drives can store thousands of images at very high resolution.

8. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

9. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

10. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained

unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

COLLECTORS OF CHILD PORNOGRAPHY

11. Individuals who are interested in child pornography may want to keep the child pornography files they receive for use in the future. Individuals who collect child pornography may go to great lengths to conceal and protect from discovery their collections of illicit materials. They often maintain their collections in the privacy and security of their homes or other secure location. Additionally, individuals who utilize social media are known to keep their electronic media with them, including at their homes.

12. Individuals who collect child pornography may seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also may help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, mail, email groups, bulletin boards, IRC, newsgroups, instant messaging, Peer to peer programs, and other similar vehicles.

13. Individuals who collect child pornography may maintain stories, books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of

sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals may keep these materials because of the psychological support they provide.

14. Individuals who collect child pornography may keep names, e-mail addresses, phone numbers or lists of persons who have shared, advertised or otherwise made known their interest in child pornography or sexual activity with children. These contacts may be maintained as a means of personal referral, exchange or commercial profit. This information may be maintained in the original medium from which it was derived, in lists, telephone or address, on computer storage devices, or merely on paper.

THE INVESTIGATION

15. Beginning in or about March 2018, Investigator Mike Evans with the Okaloosa County Sheriff's Office (hereinafter "OCSO"), acting in an undercover capacity, began chatting online on the website "www.kidschat.net," in order to identify any individuals interested in exploiting or harming children. According to their publicly accessible website, Kidschat.net professes to be the "world's largest chat for kids." Kidschat.net allows its users to register for an account before chatting, or an option exists to utilize the website as a "Guest" instead. All users must click on the "I accept" button, regarding the chat room rules before being permitted to chat on their social platform. A sampling of the chat room rules are as follows:

> -You will agree to be 13 or over (not older than 19) before entering the kids chat rooms;
> -You will not post obscene or vulgar messages;
> -You will choose an appropriate and clean nickname;
> -You have finished all your homework and have some free time now; and
> -You will take breaks to rest your eyes and clear your mind.

16. On or about March 2, 2018, at approximately 12:06 a.m., an individual

with the Kidschat username "Prew654" sent a private unsolicited message to Investigator Evans, who, acting in an undercover capacity, was posing online as a 14-year-old female using the username "Amiee14." The following conversation occurred on Kidschat.net between an individual utilizing username "Prew654" and Investigator Evans, using the username "Amiee14."

Prew654: Hi age

Amiee14: 14 you

Prew654: older is that ok

Amiee14: yeah asl

Prew654: 50s m is that ok

Amiee14: Yep where u at

Prew654: USA, U?

Amiee14: Florida

Prew654: what city

Amiee14: soth walton

Prew654: what part of the state is that in

Amiee14: Walton County

Prew654: what do u looks like

Amiee14: Shot with brown hair

Prew654: eyes color height weight

Amiee14: 5 foot 100

Prew654: very pretty, any bros and sis ages

Amiee14: no

Prew654: Ever kiss a boy, you can tell me

Amiee14: No is that ok

Prew654: yea, ever had a bf[1]

Amiee14: no you wanna text somewhere else this is running slow

Prew654: what is running slow

Amiee14: this program, you wanna ****

Prew654: space that word that word is block[2]

Amiee14: K I K

Prew654: no, do u have a email

Amiee14: yeh

Prew654: can i have it

Amiee14: elfingirl@gmail

Prew654: Can u email me now

Amiee14: yeah

Prew654: happyperson2900@gmail.com

(This portion of the conversation concluded at approximately 1:00 a.m. and then switched to email and continued.)

17. On or about March 2, 2018, at approximately 1:03 a.m., Investigator Evans, still posing in an undercover capacity and using email address elfingirl2005@gmail.com, at the request of the username Prew654, sent an email to the

[1] Based on your affiant's training and experience in online investigations involving minors, the term "bf" is short for "boyfriend."

[2] Based on your affiant's training and experience with social media applications and online platforms, your affiant knows that some chat platforms will not permit words that the platform considers lewd/crude or could potentially provide another social platform for the user to use. In this circumstance, the user Prew654 is informing Amiee14 how to work around the system/platform restrictions in order to communicate.

person utilizing email address happyperson2900@gmail.com, and stated, "Hello." Within minutes, the individual using email address happyperson2900@gmail.com responded, "Hi how r u doing," and asked, "Any pics of u sweetie?" Investigator Evans responded, "Sure where do u live?" Happyperson2900@gmail.com replied, "n y can I see them?" Investigator Evans shortly thereafter emailed an image of a young female in a red and white checkered shirt. The following is a synopsized version of the conversation that ensued beginning at approximately 1:12 a.m., between Investigator Evans, using the email address elfingirl2005@gmail.com (hereinafter referred to as "EG"), and the person using the email address Happyperson2900@gmail.com (hereinafter referred to as "HP"):

HP: y r very pretty will u be my gf.[3]

EG: sure but we kind far

HP: I will come down there to see u. any more pics of u sweetie. Is that a yes u r my gf now.

EG: yes im ur gf. What u wanna do when u come down

HP: do u like water parks. Movies.

EG: yeah is that all u wanna do be honest

HP: do u want me to touch u sweetie.

Having not responded right away, HP continued inquiring by stating, "What kind of stuff do u want to do" and, "What r u doing now?"

EG: I'm looking to learn stuff I havnt done anything, is that ok?

[3] Based on your affiant's training and experience in online investigations involving minors, the term "gf" is short for "girlfriend." In this circumstance, the 50-year-old person utilizing the Gmail account in question is soliciting the 14-year-old minor to be his girlfriend.

HP: I will teach u new stuff sweetie any sexy pics of u yes or no[4]

18. At approximately 7:30 a.m. on or about March 2, 2018, the emails continued with the following:

HP: Gm sweetie.

EG: I have pics. What new stuff will u teach me

HP: I will teach u about sex and how I can please u a lot to feel good, when can I see your sexy pics sweetie. Can I kiss u sweetie

19. At approximately 4:09 p.m. on or about March 2, 2018, HP sent an email stating, "r u home from school yet?"

20. At approximately 4:37 p.m. on or about March 2, 2018, after receiving confirmation that the purported minor was home, HP sent an email stating, "Miss me sweetie," and, "Can I see some pics please?"

21. At approximately 4:52 p.m. on or about March 2, 2018, Investigator Evans, at the request of the person using email HP, and using email EG, emailed a second picture of the same young female, which depicted the female in a black and white shirt. The following emails continued between HP and EG:

HP: u r very beautiful

HP: any sexy pics yes or no

EG: "um idk."[5]

HP: Please send me one kisses baby

---

[4] It should be noted that from here on out in approximately every instance that HP writes the word "sexy," or "sex" it is intentionally spelled with a "space" somewhere within the word. Ex: "se x" and "s e xy." However, for the purposes of this transcript, the spaces have been removed.

[5] Based on your affiant's training and experience in online investigations, the term 'idk' is an abbreviation for "I don't know."

EG: I think you just want pics from me

HP: I want to spend time with you

HP: Can I see a full pic of you

HP: Will u spend the night with me

HP: Do u have a cell phone

HP: Can I take u to the new water park that opened last year

EG: Yeah I got a phone. Yes ill spend the night with u but what u wanna do?

HP: Do u want sex with me, yes or no

EG: Yes I want to learn that be kool

HP: Can I have your number?

HP: What grade r u in and when is your birthday?

EG: I'm in 8th grade and my birth day is novemver 11. Just so u know I'm deaf if that bothers u and u don't want to talk to me any more I understand

The person using email HP then commented that it did not bother him, and requested that she teach him sign language.

22. At approximately 5:45 p.m. on or about March 2, 2018, the conversation between Investigator Evans, using email EG, continued with an individual utilizing the email HP:

HP: do u have tits yet

EG: yeah that ok

HP: do u remember how old I am. Will u let me take your clothes off of u. R u still here?

EG: sry was feeding my dogs. Yes ur 50 right. And yes ill let u take my clothes off.

HP: can I get u pregnent

EG: idk

HP: am I your first bf

EG: yes

HP: r u happy with me[6]

23. At approximately 6:38 p.m. on or about March 2, 2018, HP sent an email which included a picture depicting seven adult men, dressed in formal attire, standing in front of a giant cross inside a building. (The image is similar in nature/appearance to what a typical wedding picture would look like in which the groomsmen are all posed together side by side in the front of a church.) HP asked, "Do u like what I looks like?" After Investigator Evans responded affirmatively using email EG, HP asked, "did u ever saw a cock yet?" and then, "How big r your tits?"

24. At approximately 8:08 p.m. on or about March 2, 2018, HP asked, "What kind of school do u go to. Can we take a shower together?"

25. At approximately 8:28 p.m. on or about March 2, 2018, HP asked how long she was going to be his girlfriend, to which Investigator Evans replied using email EG, "How long u want me too. U ever gonna answer my questions?" The following conversation ensued, which is synopsized below:

HP: I want u to with me forever. What questions do u want me to answer.

EG: What are u gonna teach me and how silly lol

HP: are u smiling

[6] Based on your affiant's training and experience in online investigations involving adults and minors, your affiant is familiar with adults asking questions such as, "are you happy with me," in an effort to further solicit the minor into a deeper relationship with the adult predator.

EG: yes

HP: I am going teach u how to touch me, play with my cock suck it, I am going play with your tits and pussy do u want that sweetie. Am I making u very happy

EG: yes very much

HP: r u falling in love with me

EG: idk is that ok, I cant wait for u to teach me

Several minutes later, HP asked:

HP: do u have a nude pics of u yes or no. It is ok.

EG: no I got in trouble once for it.

HP: that's ok sweetie will u be faithfully to me

EG: What do you mean

HP: will u cheat on me, go with other guys

EG: no

HP: do u have any hair on your pussy

At approximately 10:05 p.m. on or about March 2, 2018, HP asked, "Can I put my cock inside your pussy?"

EG: Yeah, is that what you want to do?

HP: I do baby.

Later on that same night, HP asked:

HP: would u be mad at me if I got u pregnant?

EG: idk. I think I might be a little young for it. Would u be mad?

HP: but if u get pregnant what will u do. Did u had a period yet?

EG: idk what I would do. What would u want me to do and yes on the other.

HP: if u get pregnant I will take care of u sweetie

EG: ok kool. Ur so sweete

HP: can I have your address?

Having not received a reply, HP asked again:

HP: Will you give to me your address?

HP: R u there?

EG: idk bout that

HP: how r we going to meet without your address

EG: I can meet u by my house and u can pick me up if that's ok

HP: that's ok but I need some kind of address to get u, don't have to be yours. What will you wear when u first meet me?

EG: what do u want me to wear

HP: skirt blouse sexy bra and panties.

26. On or about March 3, 2018, at approximately 5:56 p.m., HP continued the conversation via email, and asked if Investigator Evans, posing as a minor using email EG, had ever seen snow before and indicated that it snowed a lot where he resided. HP then asked who the minor lived with, to which Investigator Evans replied using email EG, "My mom." Three images were then emailed by HP that depicted large piles of snow. HP then inquired, "where is dad at?" Investigator Evans using email EG replied, "no dad, he left when I was yug. That looks cold." HP commented, "I will keep u warm when we cuddle together." HP then asked, "Are u going to let me take good care of u sweetie?" Investigator Evans using email EG replied, "that be great. How are you going to do that? HP responded, "After a while u will be living with me."

27. The conversation continued into the night, when at approximately 8:07

p.m. on or about March 3, 2018, HP asked if he could have the minor's phone number, and then later on asked if the minor could cook and if she kept a clean place. Having not responded, HP kept inquiring of the minor, "Sweetheart," and "are you still awake," and at approximately 11:55 p.m., "hello where did you go to?"

28. On or about March 4, 2018, HP sent Investigator Evans, using email EG, a litany of emails that went unanswered by Investigator Evans, such as:

At approximately 9:07 a.m.: "Gm what r u doing"

At approximately 10:51 a.m.: "are u awake yet"

At approximately 12:04 p.m.: "Hi"

At approximately 1:05 p.m.: "What r u doing"

At approximately 2:12 p.m.: "Hello"

At approximately 3:22 p.m.: "are u awake"

At approximately 3:54 p.m.: "r u mad at me"

At approximately 5:16 p.m.: "hey"

At approximately 6:45 p.m.: "hello where are u today"

At approximately 9:25 p.m.: "hi"

29. On or about March 5, 2018, at approximately 8:36 a.m., Investigator Evans responded using email EG, "Hi, sry was busy yesterday." HP commented, "Miss me? What r u doing now?"

30. The conversation continued via email up until on or about March 13, 2018, at approximately 8:31 a.m., when HP wrote: "Text me when u come home from school." Investigator Evans, using email EG, replied, "I don't have your phone number to text you." HP supplied cellular telephone number 727-458-3589. At approximately 4:33 p.m., Investigator Evans, using email EG, emailed, "I sent u a

text." The conversation then switched over to text communications using cellular telephone number 727-458-3589.

31. HSI Pensacola Special Agent Lindey Bosso conducted a multiple queries in both public databases, as well as in law enforcement databases, for any information regarding the subscriber of the cellular telephone number 727-458-3589, and any information which could lead to identifying the person utilizing that cellular telephone number. Special Agent Bosso determined through online public databases that cellular telephone number 727-458-3589 was geo-located out of/associated with Clearwater/St. Petersburg, Florida. In addition, Special Agent Bosso located information through law enforcement databases that Glenn VARRIN was the potential subscriber of cellular telephone number 727-458-3589, and that VARRIN resided in Syracuse, New York, which matched the information that HP provided to Investigator Evans during both the Kidschat.net chat and email communication.

32. Special Agent Bosso then conducted a driver's license query in the Driver and Vehicle Information Database for any information related to Glenn VARRIN. Your affiant located an expired driver's license record that matched the name Glenn VARRIN, and furthermore listed VARRIN'S state of birth as New York. The residential address that was associated with the expired license was 2143 20th Avenue North, St. Petersburg, Florida, which matched the approximate geo-location of cellular telephone number 727-458-3589.

33. Between on or about March 14, 2018, through May 4, 2018, the individual using cellular telephone number 727-458-3589, believed to be Glenn VARRIN, exchanged text messages with Investigator Evans, posing in an undercover capacity. As indicated in the below text messages, your affiant has learned that the

individual using cellular telephone number 727-458-3589, believed to be Glenn VARRIN, is a truck driver, as indicated by his text messages on or about March 14, 2018, and or about March 28, 2018:

March 14, 2018:

727-458-3589:	it's 84 where I am at now
EVANS:	Where u at
727-458-3589:	Phoenix Arizona for today
EVANS:	Y u there
727-458-3589:	job I drive for my job
EVANS:	Kool
727-458-3589:	ever been in a semi
EVANS:	No
727-458-3589:	would u go into one with me
EVANS:	Yeah, that be cool
727-458-3589:	do u know have beds in there. do u want to join me in bed in the truck
EVANS:	Yeah what would we do lol
727-458-3589:	we can have sex in there

March 28, 2018:

EVANS:	Where ur today
727-458-3589:	Virginia
EVANS:	Kool. What do you drive
727-458-3589:	international pro star 2019. got it two weeks ago in Phoenix az
EVANS:	Whats that

727-458-3589: a big semi truck

34. The individual using cellular telephone number 727-458-3589, believed to be Glenn VARRIN, then texted several images of a new truck, complete with images from inside the cab of the truck where the bed area is still wrapped in plastic. The truck has markings on it denoting the trucking company, "Swift."

35. On or about March 28, 2018, the individual using cellular telephone number 727-458-3589, believed to be Glenn VARRIN, continued to make his intentions known to the purported minor by sending the following text messages to Investigator Evans who was acting in an undercover capacity:

727-458-3589: how old r u again 12 13 14

EVANS: 13 u don't remember

727-458-3589: I though u was. do u want to learn French kissing

EVANS: Yeah what else u gonna teach me

727-458-3589: do u want to see my c o ck

36. On or about April 1, 2018, the individual using cellular telephone number 727-458-3589, believed to be Glenn VARRIN, sent several pictures via text messages, which included two images of a white male. In one image, the male is standing in front of a semi-truck with the "Swift" name markings on it, seemingly the same truck as described and depicted earlier in previous images sent. In the other image, the same white male with a shorter haircut is seated in a blue recliner with a dog on his lap. When compared by Special Agent Bosso to the image on the expired Florida's driver's license, the male in both of these images matches that of Glenn VARRIN. It appears to Special Agent Bosso that the individual who was utilizing the username "Prew654" on Kidschat.net, the email account Happyperson2900@gmail.com, and sending text messages using cellular telephone number

727-458-3589, is the same individual, who is attempting to solicit and entice the female minor to depart from her residence in order to engage in a sexual relationship with him.

37. On or about April 15, 2018, the individual using cellular telephone number 727-458-3589, believed to be Glenn VARRIN, informed via text message that he would be coming to visit the minor in 19 days:

EVANS: U sure u ok with my age and all

727-458-3589: your is is very fine with me. is me good for u. we going see each other in 19 days

727-458-3589: do you still want to meet me. I love u. I want to meet my love real bad. R u going meet me may 4 friday

38. On or about May 4, 2018, law enforcement established surveillance at the Emerald Coast Inn and Suites hotel located in Fort Walton Beach, Florida. The individual using cellular telephone number 727-458-3589, believed to be Glenn VARRIN, continued to communicate with an individual he believed was a 14-year-old female. Arrangements were made to meet the minor and pick her up (in his rental vehicle) for the purposes of spending the weekend together so the two of them could engage in a sexual relationship. The individual using cellular telephone number 727-458-3589, believed to be Glenn VARRIN, communicated via text message with Investigator Evans, who continued to pose as a female minor, that he (VARRIN) would be spending the night in the area on or about May 3, 2018, and he (VARRIN) had acquired a hotel room at an establishment that had the word "Emerald" in the name. Furthermore, the individual using cellular telephone number 727-458-3589, believed to be Glenn VARRIN, informed that he had dropped off his semi-truck, and had rented a black Mazda sport utility vehicle

(hereinafter "SUV"), which he would utilize as his temporary mode of transportation when picking up the minor at the designated meeting location near to her house.

39. At approximately 11:00 a.m., on or about May 4, 2018, Special Agent Bosso observed a white male, who matched the appearance of whom your affiant knows to be VARRIN (based on the images VARRIN supplied Investigator Evans as well as the driver's license photo), exiting the Emerald Coast Inn and Suites hotel and walking to a parked black Mazda SUV bearing Florida license plate JBIY14. VARRIN was wearing a dark colored shirt and khaki colored shorts. VARRIN carried a duffle bag that he placed in the rear of the vehicle.

40. Investigator Evans, while still posing as a 14-year-old female with a hearing disability, arranged to meet VARRIN around 2:00 p.m. Investigator Evans, acting in the undercover capacity, had explained that the reason was that the minor was homeschooled; that her mother came home routinely for lunch; and the minor could not leave her residence until the mother returned to work from her lunch break.

41. On or about May 4, 2018, at approximately 11:08 a.m., Investigator Evans, acting as a minor in an undercover capacity, sent a text message to the individual using cellular telephone number 727-458-3589, believed to be Glenn VARRIN, and provided the address of a nearby Tom Thumb gas station located at 1101 Eglin Parkway, in Shalimar, Florida. Investigator Evans, acting as a minor in an undercover capacity, informed VARRIN that he could pick-up the female minor at this location, because it was allegedly in walking distance from her residence. At approximately 11:30 a.m., your affiant followed VARRIN as he departed the hotel in the black Mazda SUV, but not before he communicated via text message with Investigator Evans, acting as a minor, asking what her favorite colored roses were. Investigator Evans responded that pink roses were the preference.

42. Your affiant conducted surveillance of VARRIN as he exited the hotel parking lot and drove towards the direction of the purported minor. VARRIN was observed driving as he turned onto a road that led to a Publix grocery store, but was not followed to the store itself.

43. Special Agent Bosso continued driving towards the Tom Thumb gas station and set-up in close proximity to it, in order to observe VARRIN, in the black Mazda, as he approached. Between approximately 12:30 p.m. and 1:00 p.m., Special Agent Bosso observed VARRIN drive by the Tom Thumb on several occasions. During one drive-by of the meeting location, VARRIN waited in the left-hand turn lane (opposite the gas station) for the traffic light to signal him to turn left across traffic. However, before getting a green light to turn left, VARRIN pulled back into traffic and continued to pass by the location. Based on Special Agent Bosso's training and experience, it appeared VARRIN was conducting counter-surveillance in an effort to determine if he was being set-up by law enforcement so that he could avoid potential arrest.

44. At approximately 1:10 p.m., Investigator Evans texted VARRIN, acting in an undercover capacity as a 14-year-old minor, and informed VARRIN that she would begin walking from her house to meet him at the Tom Thumb gas station. At approximately 1:20 p.m., VARRIN was observed pulling into the Tom Thumb gas station, while driving the black Mazda SUV, and shortly thereafter, exited the vehicle. At that time, law enforcement with the Okaloosa County Sheriff's Office confronted VARRIN and arrested him.

45. Pursuant to his arrest, VARRIN'S rental vehicle was inventoried. Law enforcement located pink roses in the floorboard of the backseat, as well as bags of clothing, condoms, and generic Viagra pills. VARRIN also had with him three (3) electronic devices, that can be utilized for electronic communication.

46. VARRIN was transported to the Okaloosa County Sheriff's Office. After providing him with *Miranda* warnings, VARRIN agreed to speak with Special Agent Bosso and Investigator Evans. VARRIN was informed that the parents of the minor, with whom he had been communicating with and was scheduled to meet that afternoon, had contacted law enforcement and advised them of the situation. VARRIN was provided documents which reflected the Kidschat.net conversations VARRIN had with the purported 14-year-old minor. In response, VARRIN stated he recognized the conversation, but informed law enforcement that he was not familiar with the username "Prew654." Investigator Evans showed VARRIN a different document, which depicted a portion of a conversation when Kidschat username "Prew654" provided an email address of happyperson2900@gmail.com, and instructed the minor to email him. In response, VARRIN was asked if happyperson2900@gmail.com was an email address that belonged to him. VARRIN indicated it was. VARRIN also informed law enforcement that, when he leaves his truck rig, he carries his personal electronics with him due to his fear that they may be stolen if left inside the truck. VARRIN stated that he utilizes his IPAD when he chats online, and provided his passcode to access the IPAD. VARRIN admitted that cellular telephone number 727-458-3589 belonged to him, and that law enforcement was currently in possession of his cellular device since they removed it during the time he was arrested. It should be noted that this is the same cellular telephone number referenced in paragraph 20 that the individual believed to be VARRIN provided to Investigator Evans. It is also the same cellular telephone number that Investigator Evans was sending/receiving text messages to/from when communicating with the individual believed to be VARRIN who was interested in having sexual relations with a child. When asked where he intended to spend the night that evening with the minor, VARRIN mentioned the nearby location of Panama

City, Florida. When asked if he had already reserved a room for the evening, VARRIN stated that he had not, but that he was going to book a hotel room that evening online. (VARRIN motioned with his fingers as if he were typing on a laptop.)

47. Following VARRIN'S arrest by local authorities, SA Bosso applied for and was granted multiple Federal search warrants for the electronic devices (an IPAD, a Samsung cellphone, and a Samsung laptop computer), that were located amongst VARRIN'S possessions and found in the vehicle he was utilizing during the time in which he was apprehended for traveling to meet with a purported minor.

48. On May 9, 2018, a U.S. Magistrate Judge within the Northern District of Florida authorized the search and seizure of the electronic items that belonged to VARRIN to determine if any evidence of this crime (traveling to have sex with a minor/solicitation of a minor), or any evidence of any additional crimes related to the exploitation of minors would be located on any of the devices.

49. On May 9, 2018, the three warrants authorizing the search of VARRIN'S electronic devices (one for each item: IPAD; Samsung cellphone; Samsung laptop computer) were executed and Aaron Davis, an HSI Certified Forensic Analyst (CFA). CFA Davis was able to successfully extract content from each of the devices. Upon initial review of the forensic extraction as it related to VARRIN'S cellphone, SA Bosso reviewed the contents and located evidence of the chat communications that took place between VARRIN and Investigator Evans, posing as a 14-year-old female named "Emma." The cellular text messages exchanged between VARRIN and Investigator Evans were forensically located on the cellphone and according to the forensic extraction of the device, the communications began on or about March 13, 2018, which is the same date in which the communications swapped from the social media webpage Kidschat.net to text based cellular

communications. According to the forensic extraction of the cellphone, forensic evidence revealed that VARRIN had saved the image of the young female girl who was purporting to be a 14-year-old named "Emma," to his (VARRIN'S) cellphone "Gallery." Based on your affiant's training and experience with online investigations, your affiant knows that typically when an image is sent via text message to another user on a cellular device, the image is stored within the text communication from which it is sent. A user then must selectively hold their finger on a particular image and press the "SAVE" option when prompted, or another feature (such as "DOWNLOAD TO CAMERA ROLL") enabling the image to save to the device's camera gallery. This is commonly done so by users who do not want to lose an image accidentally or have it erased or removed from the device when the text thread is deleted. According to the cellphone forensic extraction, VARRIN also had "Emma" saved as one of his phone contacts. Also located on VARRIN'S cellphone, more specifically on the SD card within the cellphone, was a child pornography video lasting approximately 45 seconds in duration. The video was found in allocated space, which based on your affiant's training and experience, your affiant recognizes that the term "allocated space" refers to the un-deleted portion of the device, that is to say that, this child pornographic video was found on the cellphone and had not been deleted in any fashion. The video depicts a prepubescent female, who is lying on her back nude but wearing thigh-high leggings, vaginally penetrated by an adult male who then ejaculates on her.

50. Also located on the cellphone are some of the same images that VARRIN sent to Investigator Evans, not nefarious in nature, but further demonstrate that the cellphone belonged to and was utilized by VARRIN, such images include ones that depicted VARRIN'S truck rig, images of VARRIN sitting in a recliner at a residence, and images of snow-covered roads like the ones VARRIN had previously sent the purported minor. Of

equal concern, in addition to the child pornography video that was located, VARRIN had dozens and dozens of pictures (image files), of whom S/A Bosso believed were underage children, that were stored on VARRIN'S cellphone and were likely created as a result of VARRIN visiting the Kidschat.net webpage and communicating with minors online. (The forensic file path for these particular images denotes the pathway: shared/1/kids.chat/fperfil_139203963_g.jpg.) The Kidschat.net communication itself does not appear to have been stored on the actual cellphone device, so it is not known what VARRIN was discussing with those who appear to be minors. (This is likely due to the fact that VARRIN was chatting on a website/webpage versus utilizing a cellular based social media application (for example) which tends to store said communication on the actual device the user is using to communicate on. (It should also be noted that a picture (an image file) of what appears to be a black adult male's penis was also located in the same folder structure forensically as was the photos of what appears to be underage children on the Kidschat.net platform, indicating that the photos of the kids and the photo of the adult male penis were all traded/shared on the same online platform, in this case, Kidschat.net.

51. CFA Davis and SA Bosso also forensically examined and reviewed the contents of the two remaining devices authorized to search, the IPAD and the Samsung laptop computer. Once reviewed, the IPAD, although it was exempt of child exploitive material, was found to have an "Apple ID" of: "happyperson2900@gmail.com," and is the same email address VARRIN admitted to utilizing, during his post-Miranda statement to law enforcement officers, as the email account he utilized when chatting with who he believed was a 14 year old female and with who he was also intending on picking up and transporting with him out of town for the weekend. A forensic review of the IPAD'S web history revealed VARRIN searching for things to do in Panama City, Florida, such as

researching a nearby waterpark as recently as the night before VARRIN was taken into custody. (In his post-Miranda statement, VARRIN admitted to wanting to take the minor with him away for the weekend and mentioned visiting a water park as one of the things they would likely do, while they were out of town.) Other online internet searches found on the IPAD include those such as: "Teen chat" and "Teenage dating sites for 14 year olds." A preliminary forensic review of the Samsung laptop computer, also belonging to VARRIN and found in the vehicle VARRIN was utilizing during the time of his arrest, revealed a child pornography file stored on the hard drive of the device. The video file, approximately 1 minute and 3 seconds in duration, depicts a young female child performing oral sex on an adult male. Additional child exploitive material, at least six images, were also forensically located on the hard drive of the laptop computer, seemingly in unallocated space, that is, the location/space on the computer device where files which have been deleted by the user commonly reside/remain until deleted permanently by the user and/or the operating system.

52. On May 17, 2018, HSI Syracuse Special Agent Michael J. Ball and Task Force Officer (TFO) Edgar Lorenzo went to Glenn VARRIN'S last known address at 168 Parkside Avenue, Syracuse, New York and spoke with Amanda DAVIS. DAVIS advised she resides at the residence with her five (5) year old son and her boyfriend, John ELICKY, who rents the house from VARRIN. DAVIS advised that VARRIN had a room on the third floor of the residence where VARRIN stayed and kept his belongings. When asked if VARRIN had any electronics in the residence, DAVIS advised that VARRIN had a computer and a tablet that he kept in his room. After speaking with DAVIS, SA Ball then contacted ELICKY via telephone (315-813-4590). During the call, ELICKY advised that he rented the entire house from VARRIN, but that VARRIN had a locked room in the house that VARRIN kept belongings in, including a computer and a tablet. ELICKY stated that

VARRIN stayed in that room three (3) to four (4) days per month. ELICKY advised that he had been contacted by VARRIN on or about Sunday, May 13, 2018, via telephone. VARRIN requested that ELICKY go into VARRIN'S room and retrieve some paperwork to put certain bills (cable, electrical, etc.) into ELICKY'S name. ELICKY complied with VARRIN'S request and entered VARRIN'S room by removing the screws that held the locking latch on the door. While in the room, ELICKY observed a computer and a tablet. ELICKY has since received a key for the lock from VARRIN'S sister.

53. The residence is as a white with blue trim single family residence, located at 168 Parkside Avenue, Syracuse, New York. The residence is on the north side of Parkside Avenue, between Onondaga Avenue and Onondaga Park Drive. The driveway is on the east side of the residence. Entry is made into the house from the main entrance on the east side of the residence. Outside the main entrance is a small covered/open air porch. The main entrance has a white entry door which opens inward. Past the main door is a small foyer/mud room followed by a secondary door, which leads into the residence. Across from the secondary door is a carpeted stairway consisting of approximately ten (10) stairs, followed by a small landing. From the landing there is a second stairway facing the opposite direction of the first stairway, consisting of approximately five (5) steps which brings you to the second floor of the residence. The second floor consists of four (4) rooms and a stairway that leads to VARRIN'S room. The stairway has a white door with a hinged latch that is locked. The latch and lock are silver/chrome in color. The latch attaches to the door frame with three (3) black colored screws and one (1) silver/chrome colored screw, and attaches to the door with a locking mechanism.

54. In sum, the investigation confirms that VARRIN utilized the Kidschat.net online platform while on his cellular device, as well as his Gmail email account, and cellular

telephone number 727-458-3589 in order to communicate with whom he believed was an underage female minor. A forensic review of the cellular device that VARRIN had in his possession during the time of his arrest confirmed that it was his cellular device that was communicating with Investigator Evans, who was purporting to be a 14-year-old female minor, as evidenced by the forensically retrieved text communications. Additional material located on the IPAD (VARRIN'S Apple ID: "Happyperson2900") matched the same online email handle as was utilized when VARRIN exchanged email communications with who he believed was a 14-year-old minor and was repeatedly soliciting for a sexual relationship during the months of communicating. Furthermore, the presence of child pornography files found forensically on both his cellular device and laptop computer, coupled with the fact that additional images of unknown children, in the form of what appears to be profile pictures (like one would have on a social media page) having derived from the Kidschat.net website which predominately caters to youth, that VARRIN admitted to frequently visiting and communicating on, your affiant submits that there is probable cause to believe that evidence of this attempted enticement of a minor or other attempted enticements of other potential minors and/or that child pornography images and/or videos, similar to the ones stored/maintained on VARRIN'S electronic devices that traveled with him from his residence in New York to the Northern District of Florida where they were searched and seized, will be located/stored on electronic devices located in VARRIN'S room located on the third floor of 168 Parkside Avenue, Syracuse, New York. In addition, based upon the requests for nude images of the person whom he believed to be an underage female minor, as referenced above, your affiant submits that there is probable cause to believe that evidence of possession of child pornography will be located/stored on the electronic devices observed in VARRIN'S room.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

55. I have spoken with law enforcement personnel trained in computer evidence recovery who have knowledge about the operation of computer systems and the correct procedures for the seizure and analysis of computer systems.

56. These individuals have participated in the execution of numerous search warrants during which they have seized and/or examined computer systems. These individuals have also participated in several warrants that involved the search and/or seizure of, and has been responsible for analyzing, seized electronic data and records from those systems.

57. Based on my experience and training, plus the common sense knowledge that in today's technological world, computers and computer related media are used for communication and storage of data and information. As such, it is reasonable to believe that some or all of the records sought to be seized will be in electronic/digital format.

58. Furthermore, based upon my training, experience, and consultations with law enforcement personnel who specialize in searching computer systems, I have learned that searching and seizing information from computer systems and other storage media (including PDAs, cell phones, MP3 Players, etc.) often requires agents to seize most or all the computer system or storage media to be searched later by a qualified computer forensic examiner in a laboratory or other controlled environment. This is true for the reasons set out below.

59. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. The hard drives commonly included in mere desktop computers are capable of storing millions of pages of text; the storage capacity

of other electronic devices (e.g. a micro drive, a thumb drive, etc.) can also be significant. Unlike the search of documentary files, computers store data in "files" that cannot easily be reviewed. For instance, a single 1 gigabyte of storage media is the electronic equivalent of approximately 500,000 pages of double spaced text. Most computer and electronic devices have capacities well in excess of a single gigabyte.

60. The search through the computer (or other electronic media) itself is a time consuming process. Software and individual files can be "password protected." Files can be placed in hidden directories; files can be mislabeled or be labeled with names that are misleading. Similarly, files that contain innocent appearing names ("Smith.ltr") can in fact be electronic commands to electronically cause the data to self-destruct. Also, files can be "deleted," but, unlike documents that are destroyed, the information and data from "deleted" electronic files usually remains on the storage device until it is "over written" by the computer. For example, the computer's hard drive stores information in a series of "sectors," each of which contains a limited number of electronic bytes usually 512. These sectors are generally grouped to form clusters. There are thousands or millions of such clusters on a hard drive. A file's clusters might be scattered throughout the drive (for example, part of a memo could be at Cluster 163, while the next part of the memo might be stored at Cluster 2053). For a non-deleted file, there are "pointers" that guide the computer in piecing the clusters together. For a file that has been deleted, the "pointers" have been removed. Therefore, the forensic examination would include the piecing together of the associated clusters that made up the "deleted" file. Being aware of these pitfalls, the investigator/analyst must follow a potentially time-consuming procedure to review the contents of the computer storage device so as to insure the integrity of the data and/or

evidence. A single computer and related equipment could take many days to analyze properly.

61. Computer storage media are used to save copies of files and communications, and printers are used to make paper copies of these communications and files. Applications and associated data stored on the storage media are the means by which the computer can send, print and save such activity. Finally, password protected data and other security devices are often used to restrict access to or hide computer software, documentation or data. All these parts of a computer are integrated into the entire operation of a computer. In order to evaluate the evidence most effectively, the computers and all of the related computer equipment described above should be available to a computer investigator/analyst.

62. Therefore, based upon my knowledge, training, and experience, as well as information related to me by Special Agents and others involved in forensic examination of computers, I am aware that searches for and seizures of evidence from computers commonly require Agents to seize most or all of a computer system's input/output and peripheral devices (including other storage media), in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. In order to fully retrieve data from a computer system, investigators must seize all the storage devices, as well as the central processing units (CPUs), and applicable keyboards and monitors which are an integral part of the processing unit.

63. Furthermore, searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have

specific expertise in the type of computer, software application or operating system that is being searched.

64. The best practices for analysis of computer systems and storage media rely on rigorous procedures designed to maintain the integrity of the evidence and to recover hidden, mislabeled, deceptively named, erased, compressed, encrypted, or password protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment, such as a law enforcement laboratory, is typically required to conduct such an analysis properly.

65. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

66. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a) on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;

b) examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c) searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d) surveying various file directories and the individual files they contain;

e) opening files in order to determine their contents;

f) scanning storage areas;

g) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

h) performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

67. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2252 and 2252A and 2422(b), is located in the Subject Premises and within computers, computer equipment and/or other electronic media located therein.

68. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of (A) Varrin's room which is located inside a residence at 168 Parkside Avenue, Syracuse, New York and (B) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or

transmitting digital data or digital media that are located during the course of said searches, for the items listed in Attachment B.

Michael J. Ball, Special Agent
Homeland Security Investigations

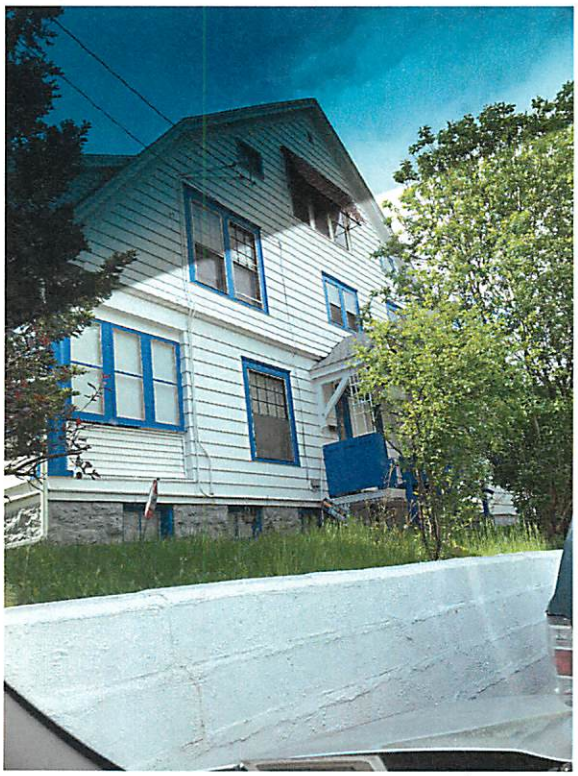
Subscribed and sworn before me
this 25th day of May 2018.

Hon. Thérèse Wiley Dancks
United States Magistrate Judge

ATTACHMENT A
PLACES AND ITEMS TO BE SEARCHED

The places and items to be searched are (A) Varrin's room which is located inside a residence at 168 Parkside Avenue, Syracuse, New York and (B) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media that are located during the course of said search.

The residence is described as a white with blue trim single family residence, located at 168 Parkside Avenue, Syracuse, New York. The residence is on the north side of Parkside Avenue, between Onondaga Avenue and Onondaga Park Drive. The driveway is on the east side of the residence. Entry is made into the house from the main entrance on the east side of the residence. Outside the main entrance is a small covered/open air porch. The main entrance has a white entry door which opens inward. Past the main door is a small foyer/mud room followed by a secondary door, which leads into the residence. Across from the secondary door is a carpeted stairway consisting of approximately ten (10) stairs, followed by a small landing. From the landing there is a second stairway facing the opposite direction of the first stairway, consisting of approximately five (5) steps which brings you to the second floor of the residence. The second floor consists of four (4) rooms and a stairway that leads to VARRIN'S room. The stairway has a white door with a hinged latch that is locked. The latch and lock are silver/chrome in color. The latch attaches to the door frame with three (3) black colored screws and one (1) silver/chrome colored screw, and attaches to the door with a locking mechanism.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items of evidence in violation of Title 18 USC §§ 2252 and 2252A (transporting, distributing, receiving, or possessing child pornography) and 2422(b)(enticement or attempted enticement of a minor) :

Computers and Electronic Media

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and electronic media will be conducted in accordance with the affidavit submitted in support of this warrant.

2. Computer hardware, meaning any and all computer equipment, including any electronic storing devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing, or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems, software, application software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data, whether themselves in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data, or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents and materials referencing or relating to the above described offenses. Such records, documents or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as thumb drives, flash drives, sd (secure digital) cards, floppy diskettes, hard disks, CD-ROMs, DVDs, optical disks, printer buffers, soft cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), or any computer or computer system. The form that such information might take includes, but is not limited to, thumb drives, flash drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, DVDs, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding, on computer media, or on media capable of being read by a computer or computer-related equipment, such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, removable hard disk cartridges, CDs, DVDs, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records

9. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored or maintained), books, notes, and reference materials.

10. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

11. Records of address or identifying information for the target of the investigation and any personal or business contacts or associates of his, (however and wherever written, stored or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user ID's, eID's (electronic ID numbers) and passwords.

12. Documents and records regarding the ownership and/or possession of the searched premises.

13. Computer records and evidence identifying who the particular user was who received, downloaded, possessed, or accessed with intent to view any child pornography found on any computer or computer media (evidence of attribution), or who attempted to do any of the foregoing, and how the computer was used to effectuate that activity.

Materials Relating to Child Erotica and Depictions of Minors

14. Any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors.

15. Any and all chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.

16. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18 United States Code, Section 2256(2).

17. Any and all notebooks and any other records reflecting personal contact, and any other activities, with minors who may be visually depicted while engaged in sexually explicit conduct, or engaged in sexually explicit chat, email, or other communications.

18. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, notes, and sexual aids.

19. Physical evidence related to the Subject Offenses, including, but not limited to clothing, personal belongings, and devices and articles which may be used to engage in sexually explicit conduct with minors

Materials Relating to Enticement of Minors

20. Any communications with minors or communications with adults regarding minors;

21. Any information pertaining to any individual's sexual interest in minors;

22. Any information in digital or hard-copy format regarding the use of Kidschat.net and the username "Prew654".

23. Any personal ads posted on any web site or in any physical newspaper or publication.

24. Any items, images, documents, communications, records, and information pertaining to the sexually explicit communications with minor(s) or adult(s) in relation to minors that

affected or were transmitted or received via computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail, including:

25. Envelopes, letters, and other correspondence including, electronic mail, chat logs, and electronic or. other instant messages, establishing possession, access to, effect on, or transmission through interstate or foreign commerce, including by United States mail or via computer, of child pornography or visual depictions of minors engaged in sexually explicit conduct;

26. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind affecting interstate or foreign commerce or involving the transmission via interstate or foreign commerce, including by U.S. mail or by computer, of any communications regarding a sexual interest in minors;

27. Credit card information, including bills and payment information, regarding Internet service; purchase of computer hardware, software, or storage media; purchase of or payment for memberships to web sites and/or chat applications;

28. Any items such as contraceptives that could be used to engage in sexual activity with a minor.

29. Any items that appear to be gifts for a young minor such as stuffed animals, flowers, that could be used to gain the minor's confidence and/or trust to induce a minor to engage in sexual activity.

30. Evidence identifying the location from which sexually explicit communications were held, including date and time of such communications;

31. Any and all photos or videos that may have been sent or received as part of a text or e-mail conversation relating to sexual interest in minors, to include date and time of the receipt or send of such files;

Photographs of Search

32. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.